and shows an exemplary embodiment and/or method of the present invention which may be configured to perform the method steps of claims 15 to 23 and/or configured to be a device as claimed in claims 24 to 29. Accordingly, Applicants respectfully request approval and entry of new Fig. 2 and withdrawal of any objection to the drawings.

With respect to paragraphs two (2) and three (3) of the Office Action, guideline(s) regarding the specification are mentioned. In accordance with 37 C.F.R. § 1.121(b)(3), the Substitute Specification (including the Abstract, but without the claims) submitted herewith contains no new matter. The amendments reflected in the Substitute Specification (including Abstract) are to conform the Specification and Abstract to U.S. Patent and Trademark Office rules or to correct informalities. As required by 37 C.F.R. § 1.121(b)(3)(iii) and § 1.125(b)(2), a Marked Up Version Of The Substitute Specification comparing the original Specification of record (before entry of amendments to Specification submitted in Applicants' Preliminary Amendment dated December 1, 1998) and the Substitute Specification also accompanies this Preliminary Amendment. In the Marked Up Version, double-underlining indicates added text and bracketing indicates deleted text. Applicants respectfully request entry of the Substitute Specification (including Abstract).

With respect to paragraphs four (4) and five (5) of the Office Action, claims 15 to 29 have been rejected under 35 U.S.C. § 112, first paragraph, as nonenabling. Specifically, claim 22 was rejected because the Specification purportedly does not state "a third number of [clock] pulses." The Specification has been amended accordingly to include "a certain number of clock pulses, for example, a third number of pulses of the clock". No new matter has been added. Specifically, the claims have been rejected for stating that certain features are "downstream". The Specification has been amended accordingly to include "downstream, that is, after," to further elucidate the term downstream. No new matter has been added. Specifically, claim 29 has been rejected because the Specification purportedly does not state that counters are subdivided or reduced. The Specification has been amended accordingly. No new matter has been added. Specifically, claim 24 has been rejected because the Specification purportedly does not state a non-linear feedback shift register. The Specification has been amended accordingly. No new matter has been added.

Accordingly, Applicants respectfully submit that the claims 15 to 29 are enabled and respectfully request withdrawal of the rejection of claims 15 to 29 under 35 U.S.C. § 112, first paragraph.

It is not clear, from the language of the Office Action, whether an enablement

rejection was confused with a written description rejection. In either event, the Specification has been amended to further clarify the features specified by the Office Action.

To the extent that the rejections concern enablement under the first paragraph of 35 U.S.C. § 112, it is respectfully submitted that the Office Action's assertions presented do not reflect the standard for determining whether a patent application complies with the enablement requirement that the specification describe how to make and use the invention -- which is defined by the claims. (See M.P.E.P. § 2164). The Supreme Court established the appropriate standard as whether any experimentation for practicing the invention was undue or unreasonable. (See M.P.E.P. § 2164.01 (citing Mineral Separation v. Hyde, 242 U.S. 261, 270 (1916); In re Wands, 858 F.2d. 731, 737, 8 U.S.P.Q.2d 1400, 1404 (Fed Cir. 1988))). Thus, the enablement test is "whether one reasonably skilled in the art could make or use the invention from the disclosures in the patent coupled with information known in the art without undue experimentation." (See id. (citing United States v. Teletronics, Inc., 857 F.2d 778, 785, 8 U.S.P.Q.2d 1217, 1223 (Fed. Cir. 1988))). In short, the Office Action's arguments and assertions do not satisfy the evidentiary and judicial standards.

To the extent that the rejections concern the written description requirement, the Examiner has the initial burden of presenting "evidence or reasons why persons skilled in the art would not recognize in an applicant's disclosure a description of the invention defined by the claims." (See M.P.E.P. § 2163.04 (citing In re Wertheim 541 F.2d 257, 262, 265, 191 U.S.P.Q. 90, 96, 98 (C.C.P.A. 1976))) (emphasis added). The Manual of Patent Examining Procedure also provides that if an examiner rejects a claim based on the lack of a written description, the examiner should "identify the claim limitation not described" and provide "reasons why persons skilled in the art would not recognize the description of this limitation in the disclosure of the application." (See id.).

With respect to paragraphs six (6) and seven (7) of the Office Action, claims 15 to 29 were rejected under 35 U.S.C. § 112, second paragraph, as indefinite.

Claim 15 has been rejected regarding the input data and steps performed. Applicants respectfully submit that the Substitute Specification at page 3, lines 5 to 16, for example, clarifies this feature. Claim 18 has been rejected regarding the "different contents of the counters". Applicants respectfully submit that the Substitute Specification at page 3, lines 18 to 31, for example, clarifies this feature and that this term is recognized by one of ordinary skill in the art. Claim 21 has been rejected regarding "outputting bits". Applicants respectfully submit that the Substitute Specification at page 4, line 9 to page 5, line 21, for example, clarifies this feature and that this term is recognized by one of ordinary skill in the

art. Claim 24 has been rejected regarding the non-linear feedback shift register and has been amended accordingly. Applicants thank the Examiner for the suggestion to correct. Claim 25 has been rejected regarding the additional feedback being tapped off. Applicants respectfully submit that the Substitute Specification at page 3, lines 5 to 16 and page 4, for example, clarifies this feature and that this term is recognized by one of ordinary skill in the art. Claims 26 and 27 have been rejected regarding its term "read off". Applicants respectfully submit that the Substitute Specification at page 3, lines 5 to 16 and page 5, for example, clarifies this feature and that this term is recognized by one of ordinary skill in the art. Claim 28 has been rejected regarding its term "XOR sum". Applicants respectfully submit that the Substitute Specification at page 4, lines 17 to 23, for example, clarifies this feature and that this mathematical term is recognized by one of ordinary skill in the art. Claim 29 has been rejected regarding its term subdividing or reducing counters. Applicants respectfully submit that the Substitute Specification at page 3, lines 5 to 16, for example, clarifies this feature and that this term is recognized by one of ordinary skill in the art. Accordingly these claims are allowable.

The remaining claims depend from either claim 15 or claim 24 and therefore are allowable for the same reasons.

In summary, it is respectfully submitted that all of claims 15 to 29 of the present application are allowable at least for the foregoing reasons.

## CONCLUSION

In view of all of the above, it is believed that the objections to the drawings, and rejections of claims 15 to 29, under 35 U.S.C. § 112, first and second paragraphs, have been obviated, and that these currently pending claims are allowable. It is therefore respectfully requested that the rejections be reconsidered and withdrawn, and that the present application issue as early as possible.

The Examiner is respectfully encouraged to contact the undersigned via telephone if such communication might advance allowance of the present application.

Respectfully Submitted,

By Linda Study
LINDA STUDY
Reg No 47084

Dated: March 25, 2002

By: Richard L. Mayer
Richard L. Mayer (Reg. No. 22,490)

KENYON & KENYON
One Broadway
New York, NY 10004
(212) 425-7200

**CUSTOMER NO. 26646**

**Amended Version Showing Changes Made**
**U.S. Application Serial No. 09/202,024**
**Attorney Docket No. 2345/45**

**IN THE CLAIMS:**

Please amend claim 24 without prejudice as follows:

24. A device for loading input data into a program when performing an authentication using a cryptographic MAC function, the device comprising:

a first counter;

a linear-feedback shift register having a nonlinear feed-forward function for reading off from the linear-feedback shift register, and for influencing an output of the linear feedback shift register using the counter, the linear-feedback shift register forming at least part of a circuit;

at least one second counter for performing the program, the at least one second counter connected downstream of the linear-feedback shift register; and

at least one additional non-linear feedback shift register for cryptographically enhancing the circuit and being connected to the circuit, the at least one additional nonlinear feedback shift register being disconnectable.

[2345/45]

# Method and Device For Loading Input Data into a[n Algorithm] Program When Performing an Authentication

## Field of the Invention

The present invention relates generally to a method [as described in detail in the preamble to Claim 1, and to a device of the kind defined in the preamble to Claim 9. Various known methods of this kind]for loading input data into a program when performing an authentication, and, in particular, to a method for loading input data into a program when performing an authentication between electronic cash cards and a security module.

## Related Technology

Various prior methods are used for electronic cash cards in a plurality of variants, [and the]with devices [are]being based on, [inter alia]among other things,[ on] chip circuits as [described by EP 0 616 429 A1.

Methods of the kind referred to here are known, for example, from]purportedly referred to by European Patent Application Number 0 616 429.

Related methods may be described, for example, in ETSI D/EN/TE 090114, Terminal Equipment (TE) Requirements for IC Cards and Terminals for Telecommunication Use, Part 4 - Payment Methods, version 4, of February 7, 1992, and [from]in the European Patent Application Number 0 605 070.

In addition to phone cards, which have a defined initial credit balance as a payment means for card-operated phones, "electronic cash cards", which work according to the same principle, are gaining in significance as a means for paying limited amounts. In "pay with chip card" applications, a card reader module having a security module SM for verifying the card and the balance amount are integrated in the automatic machine.

**MARKED UP VERSION OF THE SUBSTITUTE SPECIFICATION**

[EP]European Patent Application Number 0 605 070 [A2 also describes]further purportedly refers to a method for transferring credit and debit amounts to and from chip cards, memory locations of a chip card having overwrite capability being divided into at least two memory [locations]areas, one of these having a "debit function", thus acting as an "electronic purse" similarly to a phone card, and the other having a "credit function" along the lines of a credit card. To replenish the "electronic purse", provision is made for cash amounts to be transferred between the areas under the secured conditions that are typical for credit cards.

To both avoid the danger of unauthorized access to the automatic teller machines and their permanently installed security modules, as well as eliminate the need for dedicated lines which are specially protected and, thus, expensive for the operator, [(P95114) proposed]in a method [whereby]described in PCT Patent Application Number 95114, prior to any cash transaction, the operator of the automatic cash machine inserts a security module having chip card functions into the automatic cash machine[ and, d]. During each cash transaction that involves a cardholder inserting his or her electronic cash card into an automatic cash machine, data areas of the chip card are first read out to permit a plausibility check and to verify the remaining credit balance[; after that]. Subsequently, an authentication is performed using the security module and a single or multiple acceptance decision is made[; and f]. Finally, the cash amount due or input is either debited to the cardholder's chip card with the aid of a security function, or added to a summing counter for cash amounts in the security module[; f]. Following the cash transactions, the counter content of the security module having chip card functions is transferred to a clearinghouse.

[T]Summary of the [object]Invention

An exemplary embodiment and/or exemplary method of the present invention is directed to[ further enhance] enhancing the security of automatic cash machines for the ["electronic]electronic cash [purses"]cards to prevent unauthorized manipulation and malfunctions.

[This object is achieved in accordance with the characterizing part of Claim 1.

Advantageous variants or further developments of this method are described in the characterizing parts of dependent Claims 2 through 8.

The characterizing part of Claim 9 describes a device which is suitable for the application of the method.

The characterizing parts of dependent Claims 10 through 14 contain advantageous variants or further developments of these devices for various applications.

The invention, including its effects, advantages and field of application, is described in detail by the following examples]Another exemplary embodiment and/or exemplary method of the present invention is directed to loading input data into an algorithm or a program when performing a cash transaction authentication between an electronic cash chip card and a security module.

Brief Description of the Drawings

Fig. 1 shows a block diagram of an exemplary method and/or embodiment according to the present invention.

Fig. 2 shows a block diagram of another exemplary method and/or embodiment according to the present invention.

Detailed Description

Fig. 1 shows a block diagram of an exemplary method according to the present invention for loading input data into a program when performing a cash transaction authentication between an electronic cash chip card and a security module, the chip card including a stored credit balance. As shown in block 102, a cash amount requested, preferably input by the cardholder, is debited from an electronic cash ship card using a security function. The requested cash amount is added and stored in a cash amount summing counter of a security module, as shown in block 104. Then, as shown in block 106, input data is subdivided into a plurality of data blocks. According to the present invention, the data blocks are loaded into a linear-feedback shift register for performing the program, the linear-feedback shift register

having at least one nonlinear function cryptographically enhanced using at least one downstream counter, as shown in block 110. Lastly, as shown in block 112, the at least one additional feedback is switched off after a predefined number of clock pulses.

Fig. 2 shows a block diagram of an exemplary device 120 according to the present invention for loading input data into a program when performing an authentication using a cryptographic MAC function. The device 120 shown includes a first counter 122. The device 120 further includes a first linear-feedback shift register 124 which may have a nonlinear feed-forward function for reading off from the first linear-feedback shift register 124 and for influencing an output of the first linear-feedback shift register 124 using the first counter 122. The device 120 further includes at least one second counter 126 for performing a program associated with the present invention, the at least one second counter 126 being connected downstream, that is, after, the first linear-feedback shift register 124. The device 120 further includes at least one additional non-linear feedback shift register 128 for cryptographically enhancing the device 120, the at least one additional non-linear feedback shift register 128 being disconnectable from the device 120. In this exemplary device 120, the first counter 122 and/or the at least one second counter 126 may be subdivided or reduced.

Authentication algorithms [are typically]may be used to enable reliable identification. Often entering into the authentication methods, besides the identity of a chip card, [of ]a person, and[ possibly of]/or a security module SM, are other data[, as well], which have to be verified. An authentication method can be applied, for example, to non-secret card data D, together with a secret key K, and a random number Z. For the sake of security when working with [the ]electronic cash cards, separate security functions [are]may be used for debiting and crediting, and each of these security functions [is]may be retrieved using a cryptographic checksum.

[The]Exemplary methods of the present invention may enable[s] the debit and credit transactions to be carried out using a cryptographic token, [the condition being]where it is required that the authentication and cryptographic checksum process are performed on the

counter content using a challenge/response method. A single challenge/response method can then be applied, whereby only one random number is provided by the security module SM and only one response is calculated by the chip card, to verify both the identity (authentication) as well as the internal counter content with respect to the security module SM.

This [can]may be achieved [in that]with the variable input data, such as the counter content and the random number, [are]being initially processed internally using "keyed hash [functions" =]functions," that is, MAC functions. In the process, the card-specific secret key of the chip card is used as the key. The two tokens extracted from the counter content and the random number [can]may then be linked together, for example, (in a perhaps cryptographically unsecured way) by XOR or [y]by using a linear-feedback shift register, and then may be output, with their integrity being protected, using a cryptographic function that is [strong enough.

This method is of practical use insofar as]sufficiently powerful.

This exemplary method of the present invention provides that the keyed hash functions, which are only used internally, do not have to meet any particularly high requirements with regard to their security, and relatively simple functions can be used since the results of these functions do not leave the chip card. Nevertheless, data manipulation [is]may be effectively prevented with this exemplary method.

[The]A further exemplary method and/or exemplary embodiment of the present invention may assume[s] that a linear-feedback shift register (LFSR) having an additional nonlinear function and downstream counters is used[:

0]. Exemplary steps and features may include that:

[A]additional feedback circuits are switched into the linear-feedback shift register LFSR following the downstream counters[.];

[1. ] [I]input data, composed of the non-secret card data D and the secret key K, are read into the linear-feedback shift register LFSR, while both the feedback of the linear-feedback shift register LFSR, as well as the additional feedback(s) are active[.];

[

2. A]

a certain number of clock pulses is processed without additional input data being read in[.

];

[3. I] input data made up of the random number R are read in while both the feedback of the LFSR and the additional feedback(s) are active[.

];

[4. T] the additional feedback circuits are switched off, and the counters are reset, if necessary[.

]; and/or

[5. A] a certain number of clock pulses, for example, a third number of pulses of the clock, is processed, and, during these pulses, output bits are generated according to the current counter settings.[

]

Abstract[ of the Disclosure

2.1The problems posed by]

A method for enhancing data security when chip cards are used for payment transactions [are encountered when]and input data are loaded into an algorithm when performing an authentication.[

2.2 ]_The security of the debit and credit data is enhanced by subdividing the data blocks and by switching an additional feedback on and off following the downstream counters at preselected [times (]clock [pulses)]pulse times.[

2.3 ]_The [invention]method is applicable to all authentication processes in conjunction with chip cards.[

]